CASKEY, ROBERT ALEXANDER. Factorization of Irreducible Polynomials over a Finite Field. (1975)
Directed by: Dr. Andrew F. Long. Pp. 25.

Let GF(q) denote the finite field of order $q = p^n$, where p is an arbitrary prime and $n \geq 1$. Q(x) will denote an irreducible polynomial of degree s over GF(q). The following two theorems describe the factorization of $Q(x^{q^r}-x)$ where r is an arbitrary positive integer:

THEOREM I: Let Q(x) be irreducible of degree s over GF(q). Let (r,s) = d, and let s = s'd and r = r'd. If $Q(x)|\rho_{s'}(x)$ then $Q(x^{q^r}-x)$ is the product over GF(q) of irreducibles of degree st, $t|r'$. The number of irreducibles of degree st is

$$\sum_{\substack{v|d \\ (t,d/v)=1}} N(vt,q)/t$$

for each $t|r'$.

THEOREM II: Let Q(x) be irreducible of degree s over GF(q). Let (r,s) = d, and let s = s'd and r = r'd. Let $r' = p^k\ell$, $(p,\ell) = 1$ and $k \geq 0$. If $Q(x)\nmid\rho_{s'}(x)$, then $Q(x^{q^r}-x)$ is the product over GF(q) of irreducibles of degree $p^{k+1}st$, $t|\ell$. For each $t|\ell$, the number of irreducibles of degree $p^{k+1}st$ is

$$\sum_{\substack{v|D \\ (t,D/v)=1}} N(vt,q)/p^{k+1}t$$

where $D = p^k d$.

FACTORIZATION OF IRREDUCIBLE POLYNOMIALS OVER A FINITE FIELD

by

Robert Alexander Caskey

A Thesis Submitted to
the Faculty of the Graduate School at
The University of North Carolina at Greensboro
in Partial Fulfillment
of the Requirements for the Degree
Master of Arts

Greensboro
1975

Approved by

Andrew E. Long, Jr.
Thesis Advisor

APPROVAL PAGE

This thesis has been approved by the following committee of the Faculty of the Graduate School at the University of North Carolina at Greensboro.

Thesis Advisor Andrew F. Long, Jr

Committee Members W. Thurston, Jr.
Hughes B. Hoyle, III
Theresa P. Vaughan

August 8, 1975
Date of Acceptance by Committee

ACKNOWLEDGMENT

The author wishes to express sincere appreciation to Dr. Andrew F. Long and Dr. L. Carlitz for their guidance and inspiration in the development of this thesis.

TABLE OF CONTENTS

INTRODUCTION

In [6] the basic definitions and theorems of abstract algebra are defined and developed. The fundamental concepts of number theory can be found in [5]. The purpose of this thesis is to survey the development of the essential ideas in [2] from the material in [1] and [3].

In Chapter I, definitions and theorems necessary for the factorization of an irreducible polynomial over a finite field GF(q) are stated. The fact that an irreducible Q(x) in GF(q) has the factorization $Q(x) = \Pi_{i=0}^{n-1} (x - \alpha^{p^i})$ is proved.

In Chapter II, some preliminary concepts and theorems are established which are necessary to prove the major theorems concerning the factorization of Q(x) in Chapter III with the substitution of $x^{q^r} - x$ for x. Most of these results are found in [1] and [3].

In Chapter III, proofs of the theorems involving the substitution $x^{q^r} - x$ with (r,s) = 1 are given in detail with examples. The general theorems involving the substitution $x^{q^r} - x$ with (r,s) = d are presented briefly in relation to the proofs where (r,s) = 1.

This work has been further generalized in [4] by Dr. Long and Dr. T. Vaughan to include . . . the factorization of Q(L(x)) where L(x) is an arbitrary linear polynomial

with coefficients in GF(q).

CHAPTER I

Definition 1: Let R be a ring. Then R is said to be a commutative ring if $a \cdot b = b \cdot a$ for all $a,b \in R$.

Definition 2: A field is a commutative ring R with unity which has more than one element and such that every non-zero element of R has a multiplicative inverse in R.

Example 1: The following represents examples of fields:

(i) Q the set of rationals with respect to $+$ and $\cdot$.

(ii) R the set of real numbers with respect to $+$ and $\cdot$.

(iii) C the set of complex numbers with respect to $+$ and $\cdot$.

(iv) GF(2)

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

(v) GF(4)

$+$	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

$\cdot$	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

Definition 3: The characteristic of a field F is the smallest non-negative integer in such that ma = 0 for all a in F. If there is no such positive integer m, F is said to have characteristic zero. Some writers speak of characteristic infinity instead of zero [6].

Definition 4: A field which contains no proper subfield is said to be prime.

Definition 5: A polynomial over a field F is an expression of the form $A = A(x) = a_0 + a_1x + \cdots + a_nx^n$ where $a_i \in F$. If $a_n \neq 0$, deg A = n. If $a_n = 1$, A is monic or primary.

Definition 6: If d is the largest common divisor of a and b, it is called the greatest common divisor of a and b and is denoted by (a,b).

Theorem 1: Euclid's division lemma. If a > 0 and b is arbitrary, there exists unique q,r such that b = qa + r where $0 \leq r < a$.

Definition 7: Two numbers a and b are called relatively prime if (a,b) = 1. It can be shown that (a,b) = 1 if and only if there exists integers x and y such that ax + by = 1.

Definition 8: Let A be monic with degree A > 0. If A = BC, degree B > 0 and degree C > 0, then A is composite. Otherwise A is prime or irreducible.

Definition 9: $A \equiv B \pmod{M}$ if and only if $M \mid A-B$.

Definition 10: Consider the polynomial domain F[x]. Let M be an arbitrary polynomail. A complete residue system

modulo M is given by the set of polynomials in F[x] of degree less than degree M. A reduced residue system is obtained by deleting those polynomials not relatively prime to M. Using addition and multiplication (modulo M) for polynomials of F[x], we can form a commutative ring denoted F[x]/M.

Theorem 2: For M = P, an irreducible which is an element of F[x], F[x]/P is a field. (This is true if and only if P is an irreducible. F[x]/P is called the stem field of P.)

Definition 11: Let $\phi(m)$ denote the number of elements in a complete residue system that are prime to m. $\phi(m)$ is called the Euler ϕ-function. We have the formula

$$\phi(m) = m \prod_{p|m} (1 - \frac{1}{p}) .$$

Example 2: Determine the number of elements in the reduced system that are prime to 6.

$$\phi(6) = 6 \prod_{p|m} (1 - \frac{1}{p}) = 6(1 - \frac{1}{2})(1 - \frac{1}{3}) = 2 .$$

Clearly, the complete reduced system consists of the elements 1 and 5.

Definition 12: The mobius function $\mu(n)$ is defined as follows:

(i) $\mu(1) = 1$,

(ii) $\mu(n) = (-1)^r$ if $n = p_1 p_2 \cdots p_r$, where the p_i are distinct primes,

(iii) $\mu(n) = 0$ if $p^2 | n$ for any prime p.

Theorem 3: If P is irreducible of degree k in $F_p[x]$ the field $F_p[x]/P$ contains exactly p^k numbers.

Suppose that a field F is given which consists of t numbers where $t = p^n$, that is, the number of elements of F is a power of the characteristic. The non-zero elements of F form a cyclic commutative group G of order $p^n - 1$. We can observe

$$\alpha^{p^n-1} = 1 \quad \text{for all} \quad \alpha \in G$$

$$\alpha^{p^n} = \alpha \ .$$

Consider the polynomial $x^{p^n} - x$ in F[x]. We have the identity

$$x^{p^n} - x = \Pi(x-\alpha)$$

the product extending over all $\alpha \in F$ [2].

Theorem 4: (E. H. Moore) Every finite field is isomorphic to some field $F_p[x]/Q(x)$, where Q(x) is an irreducible polynomial of $F_p[x]$.

Theorem 5: For every prime p and integer $n \geq 1$, the finite field $GF(p^n)$ exists.

Theorem 6: Let Q(x) be an irreducible polynomial in GF[p,x] of degree n. Then in $GF(p^n)$, Q(x) has the factorization

$$Q(x) = \prod_{i=0}^{n-1} (x - \alpha^{p^i}) \ .$$

Proof: $Q(x)$ is an irreducible in $GF[p;x]$ of degree n. Let α be a root of Q. Then in the $GF(p^n)$ we have $Q(\alpha) = 0$. Now

$$\begin{aligned}(Q(\alpha))^p &= (C_n\alpha^n + C_{n-1}\alpha^{n-1} + \cdots + C_0)^p \\ &= C_n^p\alpha^{np} + C_{n-1}^p\alpha^{(n-1)p} + \cdots + C_0^p \\ &= C_n\alpha^{np} + C_{n-1}\alpha^{(n-1)p} + \cdots + C_0 \\ &= C_n(\alpha^p)^n + C_{n-1}(\alpha^p)^{n-1} + \cdots + C_0 \\ &= Q(\alpha^p) ,\end{aligned}$$

so that $Q(\alpha^p) = Q^p(\alpha) = 0$. Thus α^p is also a root. Similarly the numbers $\alpha, \alpha^p, \alpha^{p^2}, \cdots, \alpha^{p^{n-1}}$ are also roots of $Q(x)$.

To show these roots are distinct, suppose $\alpha^{p^i} = \alpha^{p^{i+j}}$ with $0 < j < n$. This implies $\alpha^{p^j} = \alpha$ (with $0 < j < n$). (It will be evident that this is impossible.) Let β represent any number of $GF(p^n)$, i.e., $\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$, an element of the residue class modulo $Q(x)$ and thus a polynomial in α with coefficients in $GF(p)$. Then

$$\begin{aligned}\beta^{p^j} &= b_0 + b_1\alpha^{p^j} + \cdots + b_{n-1}\alpha^{(n-1)p^j} \\ &= b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} = \beta .\end{aligned}$$

In other words β satisfies the equation

$$x^{p^j} = x \quad (0 < j < n)$$

which implies β can take on p^j values. Since β may take on p^n values as $\beta \in GF(p^n)$, the above equation is impossible. This proves the elements $\alpha, \alpha^p, \alpha^{p^2}, \cdots \alpha^{p^{n-1}}$ are all distinct. Hence, the factorization of $Q(x)$ is $Q(x) = \prod_{i=0}^{n-1} (x - \alpha^{p^i})$.

Example 3: Let $x^2 + x + 1$ represent a polynomial over GF(2). Clearly, 0 and 1 are not roots. If we examine GF(4) the roots are found to be α and α^2. Using the formula developed in Theorem 6 with the knowledge that α is a root of $x^2 + x + 1$

$$Q(x) = \prod_{i=0}^{n-1} (x - \alpha^{p^i}) = (x - \alpha)(x - \alpha^2)$$

$$= x^2 + x + 1 .$$

CHAPTER II

Throughout this chapter we let $q = p^n$, n a positive integer. The theorems of the preceding chapter hold if p is replaced by q.

Definition 13: If α is contained in $GF(q^s)$ but not contained in $GF(q^t)$, $1 \leq t < s$, then s is called the degree of α relative to GF(q). We use the notation deg $\alpha = s$.

Theorem 7: The number N(s,q) of elements of $GF(q^s)$ having degree s relative to GF(q) is given by

$$N(s,q) = \sum_{ij=s} \mu(i)q^j$$

where μ is the mobius function.

Example 4: N(6,q) is the number of elements of $GF(q^6)$ having degree 6 relative to GF(q)

$$N(6,q) = \sum_{ij=6} \mu(i)q^j = \mu(1)q^6 + \mu(6)q^1 + \mu(2)q^3 + \mu(3)^{q^2}$$

$$= q^6 + q - q^3 - q^2 .$$

Theorem 8: Let α belong to $GF(q^s)$. Then $x^q - x = \alpha$ is solvable in $GF(q^s)$ if and only if $\sum_{j=0}^{s-1} \alpha^{q^j} = 0$.

Proof: Necessity: Assume there exists a $\lambda \in GF(q^s)$ such that $\lambda^q - \lambda = \alpha$. Observe what takes place when the last equation is raised to successive powers of q:

$$(\lambda^q - \lambda)^q = \alpha^q = \lambda^{q^2} - \lambda^q$$

$$(\lambda^q - \lambda)^{q^2} = \alpha^{q^2} = \lambda^{q^3} - \lambda^{q^2}$$

$$\vdots$$

$$(\lambda^q - \lambda)^{q^{s-1}} = \alpha^{q^{s-1}} = \lambda^{q^s} - \lambda^{q^{s-1}} .$$

Clearly, $\sum_{j=0}^{s-1} \alpha^{q^j} = 0$ if we sum the right hand side of the above column of equations.

Sufficiency: Restating Theorem 8, (*) $x^q - x = \alpha$ is solvable in $GF(q^s)$ if and only if α satisfies the Mathiew decomposition [1]

$$\rho(x) = x^{q(s-1)} + x^{q(s-2)} + \cdots + x = 0 .$$

If x_0 is the solution of (*) the general solution is $x = x_0 + \beta$ where $\beta \in GF(q^s)$. Let $\eta = \sum_{i=0}^{s-1} \gamma^{q^i} \alpha_i$ where $\alpha_i = \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^i}$ and γ will be chosen later.

$$\eta^q = \sum_{i=0}^{s-1} \gamma^{q^{(i+1)}} (\alpha_{i+1} - \alpha) = \sum_{i=1}^{s} \gamma^{q^i} (\alpha_i - \alpha)$$

$$= \sum_{i=0}^{s} \gamma^{q^i} (\alpha_i - \alpha) = [\sum_{i=0}^{s-1} \gamma^{q^i} (\alpha_i - \alpha)] + \gamma^{q^s} (\alpha_s - \alpha)$$

$$= \sum_{i=0}^{s-1} \gamma^{q^i} \alpha_i - \sum_{i=0}^{s} \gamma^{q^i} \alpha + \gamma^{q^s} (\alpha_s - \alpha)$$

$$= \eta - \alpha \sum_{i=0}^{s-1} \gamma^{q^i} + \gamma^{q^s} (\alpha_s - \alpha)$$

$$= \eta - \alpha\rho(\gamma) + \gamma^{q^s}[\rho(\alpha)]^q$$

$$= \eta - \alpha\rho(\gamma)$$

since $\rho(\alpha) = 0$ by hypothesis. Thus $\eta^q - \eta = -\alpha\rho(\gamma)$ and by the following lemma, we may choose γ such that $\rho(\gamma) = -1$ and η is in $GF(q^s)$.

Lemma 1: There exists $\gamma \in GF(q^s)$ such that $\rho(\gamma) = -1$.

Proof: We show more generally that there exists $\gamma \in GF(q^s)$ such that $\rho(\gamma) = \alpha$ where $\alpha \in GF(q)$. By the Mathieu decomposition

$$x^{q^s} - x = \prod_{\alpha \in GF(q)} (x^{q^{s-1}} + \cdots + x^q + x - \alpha)$$

$$= \prod_{\alpha \in GF(q)} (\rho(x) - \alpha) .$$

Since $x^{q^s} - x = \Pi_{\alpha \in GF(q^s)} (x - \gamma)$, $x^{q^{s-1}} + \cdots + x^q + x - \alpha$ is a product of linear factors in $GF(q^s)$ for any $\alpha \in GF(q)$. Set $\alpha = -1$; then there exists γ such that

$$\gamma^{q^{s-1}} + \cdots + \gamma + (-1) = 0$$

since α and γ both belong to $GF(q^s)$. Thus $\rho(\gamma) = -1$ and in the preceding theorem $\eta = \Sigma\gamma^{q^i}\alpha_i \in GF(q^s)$.

Definition 14: A polynomial of the form $f(x) = \sum_{i=0}^{s} \alpha_i x^{q^i}$ is called a linear polynomial.

Note that the (ordinary) sum of two linear polynomials is a linear polynomial.

Definition 15: Let $f(x)$ and $g(x)$ be linear polynomials. The symbolic product $f \cdot g$ is given by $f \cdot g(x) = f(g(x))$

Definition 16: The linear polynomial $f(x) = \sum_{i=0}^{s} a_i x^{q^i}$ is said to correspond to the ordinary polynomial $F(x) = \sum_{i=0}^{s} a_i x^i$.

Theorem 9: If $F(x)$ and $G(x)$ are polynomials over $GF(q)$ and if $f(x)$ and $g(x)$ are the corresponding linear polynomials, then the symbolic product $f \cdot g(x)$ corresponds to the ordinary product $F(x)G(x)$.

Theorem 10: Let α be a root of the irreducible polynomial $Q(x)$ of degrees over $GF(q)$. Let $s = ds'$ and let

$$\rho_{s'}(x) = \sum_{j=0}^{s'-1} x^{q^{dj}} .$$

Then, $Q(x)$ divides $\rho_{s'}(x)$ if and only if $\rho_{s'}(\alpha) = 0$.

Proof: If $Q(x) | \rho_{s'}(x)$, then obviously $\rho_{s'}(\alpha) = 0$. If $\rho_{s'}(\alpha) = 0$, then for fixed i, $0 \leq i < s$,

$$\begin{aligned} \rho_{s'}(\alpha^{q^i}) &= \sum_{j=0}^{s'-1} \left(\alpha^{q^i}\right)^{q^{dj}} \\ &= \sum_{j=0}^{s'-1} \left(\alpha^{q^{dj}}\right)^{q^i} \\ &= \left(\sum_{j=0}^{s'-1} \alpha^{q^{dj}}\right)^{q^i} \\ &= (\rho_{s'}(\alpha))^{q^i} \end{aligned}$$

$$= 0 .$$

Thus every root of $Q(x)$ is a root of $\rho_{s'}(x)$ and $Q(x) | \rho_{s'}(x)$.

Lemma 2: Let λ be of degree s over $GF(q)$ and let γ be of degree r over $GF(q)$ with $(r,s) = 1$. Then the degree of $\lambda + \gamma$ is rs over $GF(q)$.

Lemma 3: Let α be of degree s over $GF(q)$ and let $s = ds'$, where $d = (r,s)$. If $\sum_{j=0}^{s'-1} \alpha^{q^{dj}} = 0$ then $x^{q^r} - x - \alpha$ has a root λ belonging to $GF(q^s)$.

Proof: Consider $(x^r-1, x^s-1) = x^d - 1$. Using a corollary from the Euclidean Algorithm we know there exist polynomials $A(x)$ and $B(x)$ such that

$$(*) \quad A(x)(x^r-1) + B(x)(x^s-1) = x^d - 1$$

and in terms of the corresponding linear polynomials (*) becomes

$$(**) \quad a(x)\cdot(x^{q^r}-x) + b(x)\cdot(x^{q^s}-x) = x^{q^d} - x$$

where the symbolic multiplication commutes since the coefficients belong to $GF(q)$. Recalling Theorem 8 and replacing q with q^d and s with s', there exists $\alpha \in GF(q^{ds'})$ such that $x^{q^d} - x = \alpha$ is solvable in $GF(q^{ds'})$ if and only if $\sum_{j=0}^{s'-1} \alpha^{q^{dj}} = 0$. Let $z \in GF(q^{ds'}) = GF(q^s)$ represent the solution. Then (**) becomes

$$a(z)\cdot(z^{q^r}-z) + b(z)\cdot(z^{q^s}-z) = z^{q^d} - z$$

where $(z^{q^s}-z) = 0$. Thus $[a(z)]^{q^r} - [a(z)] = \alpha$.

By closure properties of field operations $a(z) \in GF(q^s)$ since $z \in GF(q^s)$. Thus $\lambda = a(z)$ is a root of $x^{q^r} - x - \alpha$ belonging to $GF(q^s)$.

Lemma 4: Let α be of degree s over GF(q) and let $s = ds'$ where $d = (r,s)$. Suppose $r = p^k \ell d$, $(p,\ell) = 1$ and $k \geq 0$. If $\sum_{j=0}^{s'-1} \alpha^{q^{dj}} \neq 0$ then $x^{q^n} - x - \alpha$ has a root λ belonging to $GF(q^{p^{(k+1)}s})$.

Proof: $(r,p^{k+1}s) = (p^k \ell d, p^{k+1}s'd) = p^k d$ therefore $(\ell,ps') = 1$. Consider $(x^r-1, x^{p^{k+1}s}-1) = x^{p^k d} - 1$. There exists polynomials A(x) and B(x) such that the following linear combination exists:

$$(*)\quad A(x)(x^r-1) + B(x)(x^{p^{k+1}s}-1) = x^{p^k d} - 1 .$$

Substituting the corresponding linear polynomials (*) becomes

$$(**)\quad a(x)\cdot(x^{q^r}-x) + b(x)(x^{q^{p^{k+1}s}}-x) = x^{q^{p^k d}} - x .$$

We show that a solution z exists in $GF(q^{p^{k+1}s})$ which satisfies $x^{q^{p^k d}} - x = \alpha$. Let $P = q^{p^k}$ and the previous equation becomes $x^{P^d} - x = \alpha$, which has a solution $z \in GF(P^{dps'}) = GF(P^{ps})$ since $\sum_{j=0}^{ps'-1} \alpha^{P^{dj}} = p \sum_{j=0}^{s'-1} \alpha^{P^{dj}} = 0$. Substituting z in (**), $[a(z)]^{q^r} - [a(z)] = \alpha$ where $\lambda = a(z)$ is a root of $x^{q^r} - x - \alpha$ belonging to $GF(q^{p^{k+1}s})$.

Lemma 5: Let $r = r'd$. Then the set $\{tv: t|r', v|d, (t,d/v) = 1\}$ contains each divisor of r

exactly once.

Lemma 6: Let $r = p^k \ell d$ and let $p^k d = D$. Then the set $\{tv: t|\ell, v|D, (t, D|v) = 1\}$ contains each divisor of r exactly once.

CHAPTER III

Theorem 11: Let $Q(x)$ be irreducible of degree s over $GF(q)$ with the coefficient β of x^{s-1} satisfying $\beta = 0$. If $(r,s) = 1$, then $Q(x^{q^r}-x)$ is the product over $GF(q)$ of irreducibles of degree st, $t|r$. For each $t|r$ the number of irreducibles of degree st is

$$N(t,q)|t.$$

Proof: By Theorem 6 and substituting s for n,

$$(11.1) \qquad Q(x) = \prod_{j=0}^{s-1} (x-\alpha^{q^j}) \qquad (\deg \alpha = s) .$$

Substituting $x^{q^r} - x$ for x

$$(11.2) \qquad Q(x^{q^r}-x) = \prod_{j=0}^{s-1} (x^{q^r}-x-\alpha^{q^j}) .$$

Let $j = 0$ and examine the $j = 0$ factor. We have the polynomial $x^{q^r} - x - \alpha$ with root λ not belonging to $GF(q^r)$. If $\lambda \in GF(q^r)$, then $\lambda^{q^r} = \lambda$ which would imply $\alpha = 0$ and this is the trivial case. However, since λ is a root:

$$(11.3) \qquad \lambda^{q^r} = \lambda + \alpha .$$

Raising (11.3) to successive powers of q^r yields the following equations:

$$\lambda^{q^r} = \lambda + \alpha$$

$$\lambda^{q^{2r}} = \lambda + \alpha + \alpha^{q^r}$$

$$\cdots$$

$$\lambda^{q^{sr}} = \lambda + \alpha + \alpha^{q^r} + \cdots + \alpha^{q^{r(s-1)}} \tag{11.4}$$

$$\lambda^{q^{sr}} = \lambda + \sum_{j=0}^{s-1} \alpha^{q^{rj}} = \lambda \ .$$

(Observe $\sum_{j=0}^{s-1} \alpha^{q^{rj}} = -\beta = 0$ since $(r,s) = 1$.) If $\lambda = \lambda^{q^{sr}}$ then $\lambda \in GF(q^{sr})$. Observing (11.4) α is a polynomial in λ. Since degree $\alpha = s$, $s|\deg \lambda$ because $GF(q^s) \subset GF(q^m)$ if and only if $s|m$ where m is the degree of λ. Therefore the degree of λ has the form st where $t|r$ for any root λ of (11.3). Using Lemma 3 guarantees the existence of a root λ_1 of degree s relative to $GF(q)$

$$\lambda_1^{q^r} = \lambda_1 + \alpha \ . \tag{11.5}$$

$\lambda_1 + \gamma$ is also a root where $\gamma \in GF(q^r)$ thus $x^{q^r} - x - \alpha = \Pi_{\gamma \in GF(q^r)} (x - (\lambda_1 + \gamma))$ consider j^{th} factor of (11.2) $x^{q^r} - x - \alpha^{q^j}$. Taking (11.5) to q^j power yields $(\lambda_1^{q^r})^{q^j} = (\lambda_1 + \alpha)^{q^j}$ which implies $(\lambda_1^{q^j})^{q^r} = \lambda_1^{q^j} + \alpha^{q^j}$. Therefore, $\lambda_1^{q^j}$ is a root of $x^{q^r} - x - \alpha^{q^j}$. Choosing a specific $\gamma \in GF(q^r)$ let γ have degree t when $t|r$. Now (11.6) $\Pi_{j=0}^{st-1}(x-(\lambda_1+\gamma)^{q^j})$ forms one irreducible of degree st over $GF(q)$ if degree

$(\lambda_1+\gamma) = st$. We will show that this is the case and that the factors needed to form this irreducible are present in

$$(11.7) \qquad Q(x^{q^r}-x) = \prod_{j=0}^{s-1} \prod_{\gamma \in GF(q^r)} [x - (\lambda_1^{q^j}+\gamma)] .$$

For each j^{th} factor in the above expression $(\lambda_1+\gamma)^{q^j} = \lambda_1^{q^j} + \gamma^{q^j} = (\lambda_1^{q^k})^{q^{s\ell}} + \gamma^{q^j} = \lambda_1^{q^k} + \gamma^{q^j}$ where $j = s\ell + k$ $0 \leq k \leq s-1$. Thus the required factors of (11.6) are present. Now $(r,s) = 1$ implies $(t,s) = 1$. Since $\lambda_1^{q^j}$ has degree s, $0 \leq j \leq s-1$, Lemma 2 asserts that the degree of $\lambda_1^{q^j} + \gamma$ is st. For any $t|r$ the number $N(t,q)$ of γ in $GF(q^r)$ of degree t is given by Theorem 7. Since st of the factors in (11.7) are required to form an irreducible (11.6) of degree st, we have $sN(t,q)/st = N(t,q)/t$ irreducibles of degree st for each $t|r$.

Example 5: Let $Q(x) = x^3 + x + 1$, an irreducible over GF(2). Let $r = 1$ and note $\beta = 0$. Theorem 11 predicts $Q(x^2-x)$ is the product over GF(2) of irreducibles of degree 3. The number of irreducibles of degree is $N(1,2)/1 = \sum_{ij=1} \mu(i)2^j = 2$. We find that $Q(x^2-x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = (x^3+x+1)(x^3+x^2+1)$.

Theorem 12: Let Q(x) be irreducible of degree s over GF(q) with the coefficient β of x^{s-1} satisfying $\beta \neq 0$. If $(r,s) = 1$ then $Q(x^{q^r}-x)$ is the product over GF(q) of irreducibles of degree $p^{k+1}st$ where $t|\ell$ in the factorization $r = p^k\ell$, $(p,\ell) = 1$ and $k \geq 0$. The number of irreducibles

of degree p^{k+1}st is $\sum_{u=0}^{k} N(p^u t,q)/p^{k+1}t$ for each $t|\ell$.

Proof: By Theorem 6 as in previous proof

$$(12.1) \qquad Q(x) = \prod_{j=0}^{s-1} (x-\alpha^{q^j}) \qquad \text{(degree } \alpha = s)$$

and

$$(12.2) \qquad Q(x^{q^r}-x) = \prod_{j=0}^{s-1} (x^{q^r} - x - \alpha^{q^j}) .$$

Examine the $j = 0$ factor. We have the polynomial $x^{q^r} - x - \alpha$ with root λ not belonging to $GF(q^r)$ such that

$$(12.3) \qquad \lambda^{q^r} = \lambda + \alpha .$$

Since $\lambda^{q^{sr}} = \lambda + \sum_{j=0}^{s-1} \alpha^{q^{jr}} = \lambda - \beta$, $\lambda^{q^{sr}} \neq \lambda$ and $\beta \neq 0$. Therefore the following equations are produced by raising $\lambda^{q^{sr}} = \lambda - \beta$ to successive powers of q:

$$\lambda^{q^{sr}} = \lambda - \beta$$

$$\lambda^{q^{2sr}} = \lambda - 2\beta$$

$$\cdots$$

$$(12.4) \qquad \lambda^{q^{psr}} = \lambda - p\beta = \lambda \qquad \text{(since } p\beta \equiv 0 \bmod p).$$

The degree of λ is at most psr.

Since degree $\alpha = s$ and α is a polynomial in λ, α is in a subfield of the smallest field containing λ. Therefore, $s|\deg \lambda$. Let the degree of $\lambda = sm$ where $m|pr$. By (12.4)

degree $\lambda \nmid sr$. Now $sm \nmid sr$ implies $m \nmid r$. Also since $sm \mid psr$, $m \mid pr$. Let $r = p^k \ell$; $p \nmid \ell$. Hence degree $\lambda = p^{k+1} st$, $t \mid \ell$.

As in (11.4), $\sum_{j=0}^{s-1} \alpha^{q^{rj}} = -\beta$ with $\beta \neq 0$, and by Lemma a λ of minimum degree $p^{k+1}s$ does occur; call it λ_1. Then, as in the proof of Theorem 11

$$(12.5) \qquad Q(x^{q^r} - x) = \prod_{j=0}^{s-1} \prod_{\gamma \in GF(q^r)} [x - (\lambda_1^{q^j} + \gamma)] .$$

Let degree $\gamma = p^u t$ where $0 \leq u \leq k$ and $t \mid \ell$. We show that degree $(\lambda_1 + \gamma) = p^{k+1} st$ over $GF(q)$. Since $\lambda_1 + \gamma$ is a root of $x^{q^r} - x - \alpha$, we have $p^{k+1}s \mid \deg(\lambda_1 + \gamma)$. Degree $(\lambda_1 + \gamma) = p^{k+1} st'$ where $t' \mid \ell$. In fact $t' \mid t$ because both λ_1 and γ belong to $GF(q^{p^{k+1}st})$ and $\lambda_1 + \gamma$ is in a subfield $GF(q^{p^{k+1}st'})$. Now $\alpha = \theta - \lambda_1$ and

$$\gamma^{q^{p^{k+1}st'}} = \theta^{q^{p^{k+1}st'}} - \lambda_1^{q^{p^{k+1}st'}} = \theta - \lambda_1 = \gamma$$

due to the fact $GF(q^{p^{k+1}s}) \subset GF(q^{p^{k+1}st'})$. Thus $\gamma \in GF(q^{p^{k+1}st'})$ which implies degree $\gamma \mid p^{k+1}st'$ and $p^u t \mid p^{k+1}st'$. Dividing by p^u: $t \mid p^{k+1-u}st'$. Now $t \mid \ell$ and $\ell \mid r = p^k \ell$ so that $t \mid r$. Since $(r,s) = 1$ we have $(t,s) = 1$. Since $t \mid \ell$ and $p \nmid \ell$, $(p,\ell) = 1$. Then we have $(t,p) = 1$. Thus $(t, p^{k+1-u}) = 1$. By elementary number theory $(t, p^{k+1-u}s) = 1$ and therefore $t \mid t'$. Hence $t = t'$.

Note that $\lambda_1^{q^j} + \gamma$, $1 \leq j \leq s-1$, also has degree $p^{k+1}st$ over $GF(q)$ if γ has degree $p^u t$ over $GF(q)$.

Every element of $GF(q^r)$ has degree over $GF(q)$ of the form $p^u t$, $0 \le u \le k$ and $t \mid \ell$. The number of γ of degree $p^u t$ is given by $N(p^u t, q)$. Thus in the factorization (12.5) we have

$$s \sum_{u=0}^{k} N(p^u t, q)/p^{k+1} st = \sum_{u=0}^{k} N(p^u t, q)/p^{k+1} t$$

irreducibles of degree $p^{k+1} st$ over $GF(q)$.

Example 6: Let $Q(x) = x^3 + x^2 + 1$, an irreducible of degree 3 over $GF(2)$. Let $r = 2$. Since $\beta \neq 0$, $k = 1$ and $\ell = 1$, Theorem 12 predicts

$$\sum_{u=0}^{k=1} N(2^u, 2)/2^2 = [N(1,2)/4 + N(2,2)]/4 = [2+2]/4 = 1$$

irreducible polynomial of degree $p^{k+1} st = 2^2(3)(1) = 12$. We have $Q(x^4-x) = x^{12} + x^9 + x^8 + x^6 + x^3 + x^2 + 1$.

Theorem 13: Let $Q(x)$ be irreducible of degree s over $GF(q)$. Let $(r,s) = d$ and let $s = s'd$ and $r = r'd$. Suppose that $(r',d) = 1$. If $Q(x) \mid \rho_{s'}(x)$, then $Q(x^{q^r}-x)$ is the product over $GF(q)$ of irreducibles of degree st, $t \mid r'$. For eqch $t \mid r'$ the number of irreducibles of degree st is

$$\sum_{v \mid d} N(vt, q)/t \ .$$

Proof: As in the proof of Theorem 11

$$Q(x^{q^r}-x) = \prod_{j=0}^{s-1} (x^{q^r}-x-\alpha^{q^j}) \qquad (\text{degree } \alpha = s) \ .$$

Take $j = 0$. Observe that $x^{q^r} - x - \alpha$ has a root λ not belonging to $GF(q^r)$ such that

$$\lambda^{q^r} = \lambda + \alpha$$

$$\lambda^{q^{2r}} = \lambda + \alpha + \alpha^{q^r}$$

$$\cdots$$

$$\lambda^{q^{s'r}} = \lambda + \sum_{j=0}^{s'-1} \alpha^{q^{rj}} = \lambda .$$

This is a consequence of the hypothesis $Q(x) | \rho_{s'}(x)$ which is equivalent to the condition

$$\sum_{j=0}^{s'-1} \alpha^{q^{rj}} = \sum_{j=0}^{s'-1} \alpha^{q^{dj}} = 0 .$$

Since $sr' = s'r$, we have degree $\lambda | sr'$. Since α is a polynomial in λ we also have $s | \deg \lambda$. Hence the degree of λ has the form st where $t | r'$. Also, Lemma 3 guarantees that a λ of minimum degree s does occur; call it λ_1. Then, as in the proof of Theorem 11,

$$(13.1) \qquad Q(x^{q^r} - x) = \prod_{j=0}^{s-1} \prod_{\gamma \in GF(q^r)} [x - (\lambda_1^{q^j} + \gamma)] .$$

Let γ in $GF(q^r)$ have degree vt, $v | d$ and $t | r'$. With the condition $(r', d) = 1$ it can be shown that $\lambda_1 + \gamma$ has degree st. Also note that $\lambda_1^{q^j} + \gamma$, $1 \leq j \leq s-1$, also has degree st over $GF(q)$ for γ of degree vt, $v | d$ and $t | r'$.

Every γ in $GF(q^r)$ has degree of the form vt where $v | d$

and $t|r'$. The number of γ of degree vt is given by $N(vt,q)$. Since st of the factors in (13.1) are required to form an irreducible of degree st, we obtain

$$s \sum_{v|d} N(vt,q)/st = \sum_{v|d} N(vt,q)/t$$

irreducibles of degree st for each $t|r'$.

Theorem 14: Let $Q(x)$ be irreducible of degree s over $GF(q)$. Let $(r,s) = d$, and let $s = s'd$ and $r = r'd$. Let $r' = p^k\ell$, $(p,\ell) = 1$ and $k \geq 0$. Suppose that $(\ell,d) = 1$. If $Q(x) \nmid \rho_{s'}(x)$, then $Q(x^{q^r}-x)$ is the product over $GF(q)$ of irreducibles of degree $p^{k+1}st$, $t|\ell$. For each $t|\ell$, the number of irreducibles of degree $p^{k+1}st$ is

$$\sum_{v|D} N(vt,q)/p^{k+1}t$$

where $D = p^k d$.

Proof: As in the proof of Theorem 11

$$Q(x^{q^r}-x) = \prod_{j=0}^{s-1} (x^{q^r}-x-\alpha^{q^j}) \qquad \text{degree } \alpha = s .$$

Take $j = 0$. The polynomial $x^{q^r} - x - \alpha$ has a root λ not belonging to $GF(q^r)$ such that

$$\lambda^{q^r} = \lambda + \alpha . \tag{14.1}$$

Now $\lambda^{s'r} \neq \lambda$ since $\lambda^{q^{s'r}} = \lambda + \sum_{j=0}^{s'-1} \alpha^{q^{dj}}$.

Since $Q(x) \nmid \rho_{s'}(x)$ we know $\rho_{s'}(\alpha) \neq 0$. The sequence of equations

$$\begin{aligned} \lambda^{q^{s'r}} &= \lambda + \rho_{s'}(\alpha) \\ \lambda^{q^{2s'r}} &= \lambda + 2\rho_{s'}(\alpha) \\ &\cdots \\ \lambda^{q^{ps'r}} &= \lambda + p\rho_{s'}(\alpha) = \lambda \end{aligned} \tag{14.2}$$

shows that degree $\lambda \mid psr'$ since $s'r = sr'$.

As in the proof of Theorem 12 a λ of minimum degree $p^{k+1}s$ does occur; call it λ_1. Then

$$Q(x^{q^r} - x) = \prod_{j=0}^{s-1} \prod_{\gamma \in GF(q^r)} [x - (\lambda_1^{q^j} + \gamma)] . \tag{4.3}$$

Let $D = p^k d$. Suppose γ in $GF(q^r)$ has degree vt where $v \mid D$ and $t \mid \ell$. With the condition $(\ell, d) = 1$, it can be shown that $\lambda_1 + \gamma$ has degree $p^{k+1}st$ over $GF(q)$.

Also note $\lambda^{q^j} + \gamma$, $1 \leq j \leq s-1$, has degree $p^{k+1}st$ for γ of degree vt, $v \mid D$ and $t \mid \ell$.

Every element of $GF(q^r)$ has degree over $GF(q)$ of the form vt where $v \mid D$ and $t \mid \ell$. The number of γ of degree vt is given by $N(vt,q)$. Thus in the factorization of (14.2) we have

$$s \sum_{v \mid D} N(vt,q)/p^{k+1}st = \sum_{v \mid D} N(vt,q)/p^{k+1}t$$

irreducibles of degree p^{k+1}st over GF(q).

If we drop the condition (r',d) = 1 in Theorem 13, then Lemma 5 must be used in order to avoid counting some of the roots $\lambda_1^{q^j} + \gamma$ more than once (i.e. we must avoid assigning more than one value to the degree of $\lambda_1^{q^j} + \gamma$). We have

Theorem 15: Let Q(x) be irreducible of degree s over GF(q). Let (r,s) = d, and let s = s'd and r = r'd. If $Q(x) | \rho_{s'}(x)$, then $Q(x^{q^r} - x)$ is the product over GF(q) of irreducibles of degree st, $t | r'$. For each $t | r'$ the number of irreducibles of degree st is

$$\sum_{\substack{v | d \\ (t,d/v)=1}} N(vt,q)/t \ .$$

In a similar manner, Lemma 6 is used to avoid duplication in Theorem 14 when $(\ell,D) \neq 1$ necessarily. We have

Theorem 16: Let Q(x) be irreducible of degree s over GF(q). Let (r,s) = d and let s = s'd and r = r'd. Let $r' = p^k \ell$, $(p,\ell) = 1$ and $k \geq 0$. If $Q(x) \nmid \rho_{s'}(x)$, then $Q(x^{q^r} - x)$ is the product over GF(q) of irreducibles of degree p^{k+1}st, $t | \ell$. For each $t | \ell$ the number of irreducibles of degree p^{k+1}st is

$$\sum_{\substack{v | D \\ (t,D/v)=1}} N(vt,q)/p^{k+1}t \ ,$$

where $D = p^k d$.

SUMMARY

Let GF(q) denote the finite field of order $q = p^n$, where p is an arbitrary prime and $n \geq 1$. Q(x) will denote an irreducible polynomial of degree s over GF(q). The fundamental definitions and theorems of finite field theory are developed and used to prove the following two theorems:

THEOREM I: Let Q(x) be irreducible of degree s over GF(q). Let (r,s) = d, and let s = s'd and r = r'd. If $Q(x) | \rho_{s'}(x)$ then $Q(x^{q^r}-x)$ is the product over GF(q) of irreducibles of degree st, $t | r'$. The number of irreducibles of degree st is

$$\sum_{\substack{v|d \\ (t,d/v)=1}} N(vt,q)/t$$

for each $t | r'$.

THEOREM II: Let Q(x) be irreducible of degree s over GF(q). Let (r,s) = d, and let s = s'd and r = r'd. Let $r' = p^k \ell$, $(p,\ell) = 1$ and $k \geq 0$. If $Q(x) \nmid \rho_{s'}(x)$, then $Q(x^{q^r}-x)$ is the product over GF(q) of irreducibles of degree $p^{k+1}st$, $t | \ell$. For each $t | \ell$, the number of irreducibles of degree $p^{k+1}st$ is

$$\sum_{\substack{v|D \\ (t,D/v)=1}} N(vt,q)/p^{k+1}t$$

where $D = p^k d$.

BIBLIOGRAPHY

1. L. Carlitz, Unpublished notes for a course in Arithmetic of Polynomials.

2. Andrew F. Long, Factorization of irreducible polynomials over a finite field with the substitution $x^{q^r} - x$ for x, ACTA Arithmetica XXV (1973), pp. 65-80.

3. Andrew F. Long, Unpublished notes for a course in Polynomials over a Finite Field.

4. Andrew F. Long and T. Vaughan, Factorization of $Q(h(T)(x)$ over a finite field where $Q(x)$ is irreducible and $h(T)(x)$ is linear, to appear in Linear Algebra and its Applications.

5. Calvin T. Long, Elementary Introduction to Number Theory, D. C. Heath and Co., Boston, Massachusetts, 1966.

6. Sam Perlis, Introduction to Algebra, Blaisdell Publ. Co., Waltham, Massachusetts, 1966.